Matthew D. Pearson (SBN 294302)
mpearson@bakerlaw.com
BAKER & HOSTETLER LLP
600 Anton Boulevard, Suite 900
Costa Mesa, CA 92626-7221
Telephone: 714.754.6600
Facsimile: 714.754.6611

Attorney for Defendant
PRIME HEALTHCARE SERVICES, INC.

IN THE UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

R.S., individually and on behalf of all others similarly situated,

Plaintiff,

v.

PRIME HEALTHCARE SERVICES, INC.,

Defendant.

Case No.: 5:24-cv-00330-ODW-SP

DEFENDANT PRIME HEALTHCARE SERVICES, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFF R.S.'S COMPLAINT PURSUANT TO FED. R. CIV. P. 12(b)(6)

[Filed concurrently with Declaration with Matthew D. Pearson and (Proposed) Order]

Date: June 10, 2024
Time: 1:30 p.m.
Crtrm.: 5D

Complaint served: 03/04/2024
Current response date: 03/25/2024
New response date: 04/24/2024

NOTICE OF MOTION

NOTICE IS HEREBY GIVEN that on June 10, 2024, in Courtroom 5D of the United States District Court, Central District of California, located at 350 W. 1st Street, Los Angeles, California 90012, Defendant Prime Healthcare Services, Inc. ("Prime") will and hereby does move the Court for an order dismissing Plaintiff R.S.'s Class Action Complaint ("Complaint") pursuant to Fed. R. Civ. P. 12(b)(6).

This motion is made on the grounds that Plaintiff has failed to state against Prime a plausible claim for violation of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), *et seq*. More specifically:

1. Plaintiff's cause of action for violation of the ECPA should be dismissed because (1) Prime was a party to the communication allegedly unlawfully intercepted and (2) the ECPA's crime-tort exception does not apply.

This motion is made following the conference of counsel pursuant to L.R. 7-3, which took place telephonically on April 19, 2024. [*See* Declaration of Matthew D. Pearson, ¶¶ 1-5.] Following that telephonic meet and confer, the Parties were unable to reach agreement on any of the relief requested in this Motion.

This motion is based on this Notice of Motion, the accompanying Memorandum of Points and Authorities, the Declaration of Matthew D. Pearson, the Court's file and records in this action, and such other evidence and arguments as may be made or presented at or before the hearing on this Motion.

Respectfully submitted,

Dated: April 24, 2024

BAKER & HOSTETLER LLP

By: */s/ Matthew D. Pearson*
MATTHEW D. PEARSON

Attorney for Defendant
PRIME HEALTHCARE SERVICES, INC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This is not the first and likely not the last putative class action to be filed against a healthcare provider for allegedly using internet tracking technologies on its website. Over the past couple of years, hundreds of these cases have been filed.

But, as the number of these cases increased, so, too, did the certainty of the law. Courts have now held that website operators, such as Defendant Prime Healthcare Services, Inc. ("Prime") here, cannot be held liable for violating the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1), if (1) they were a party to the communication and consented to its alleged interception and (2) they did not engage in the alleged interception for the purposes of committing a crime or tort, separate and apart from the actual interception.

Of course, the path to this point has been far from a straight line, and outlier decisions do exist. But, generally speaking, courts agree that a party cannot intercept its own communications, a party can consent to the interception of its own communications, and, unless, at the time of intercepting, the party possesses the intent to commit a separate crime or tort using the intercepted communication, the crime-tort exception does not apply.

Here, there can be no dispute that Prime was a party to the communication allegedly intercepted. Plaintiff was actively sending her communications to Prime. There likewise can be no dispute that Prime consented to having its communications allegedly intercepted; it was the one who allegedly installed the trackers on its websites in the first place. And there should be no dispute that the crime-tort exception does not apply here. Not only has Plaintiff not identified a single crime or tort separate and apart from the alleged interception, but she has also failed to allege that Prime intended to commit that crime or tort at the time it allegedly engaged in the interception.

In sum, Plaintiff has failed to state a viable ECPA-violation claim against Prime. Her claim must be dismissed, in its entirety and with prejudice.

II. PLAINTIFF'S ALLEGATIONS

On February 8, 2024, Plaintiff R.S. filed a putative class action against Prime, asserting a single claim for violation of the ECPA. [*See generally* Dkt. No. 1.] Plaintiff alleges that Prime "is a privately held healthcare company established in 2011" [*id.* at ¶ 1], "is the fifth largest for-profit health system in the United States, operating 44 hospitals in 14 states, including California" [*id.*], and "owns, controls and maintains websites for its hospitals ('Websites'), as well as web-based patient portals ('Portals')" [*Id.* at ¶ 2]. Plaintiff refers to the Websites and Portals collectively as "Web Properties." [*Id.* at ¶ 2.]

Plaintiff alleges that Prime "has utilized Facebook Pixels (and, upon information and good faith belief, other tracking technologies such as Google Analytics) since at least October 2018." [*Id.* at ¶ 54.] Plaintiff further claims that Prime "installed the Meta Pixel and, upon information and good faith belief, Conversions API, as well as other tracking technologies, on many (if not all) of the webpages within its Web Properties (including the member-only patient portal) and programmed or permitted those webpages to surreptitiously share patients' private and protected communications with the Pixel Information Recipients." [*Id.* at ¶ 61.] Plaintiff claims that Prime "intentionally configured Pixels installed on its Web Properties to capture both the 'characteristics' of individual patients' communications with Prime Healthcare's Websites (their IP addresses, Facebook ID, cookie identifiers, device identifiers, and account numbers) and the 'content' of these communications (the buttons, links, pages, and tabs they click and view related to their health conditions and services sought from Defendant)." [*Id.* at ¶ 71.]

Plaintiff alleges that she "accessed Prime['s]…Web Properties on her computer and mobile devices and used the Web Properties to look for providers,

review conditions and treatments, make appointments, and communicate with her healthcare providers." [*Id.* at ¶ 30.] She further claims that she has accessed her Facebook account using these same "computer[s] and mobile devices." [*Id.*]

As a result, Plaintiff claims, "on information and belief," that Prime "intercepted and disclosed the following non-public private information to Facebook: (a) Plaintiff's…status as [a] medical patient[]; (b) Plaintiff's…communications with [Prime] through its Web Properties, including specific text queries typed into the search bar, medical conditions for which [Plaintiff] sought treatment[] and treatment[] sought; (c) Plaintiff's…searches for appointments, appointment details, location of treatments, medical providers' names and their specialties, medical conditions, and treatments; and (d) PII, including but not limited to [Plaintiff's] locations, IP addresses, device identifiers and …[her] unique Facebook ID." [*id.* at ¶ 73.]

Based on the above, Plaintiff alleges that Prime "intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff…, in violation of 18 U.S.C. § 2511(1)(a)." [*Id.* at ¶ 233.] She also claims that "[b]y intentionally disclosing or endeavoring to disclose Plaintiff's…electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), [Prime] violated 18 U.S.C. § 2511(1)(c)." [*Id.* at ¶ 237.] And she asserts that "[b]y intentionally using, or endeavoring to use, the contents of Plaintiff's…electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), [Prime] violated 18 U.S.C. § 2511(1)(d)." [*Id.* at ¶ 238.]

III. MOTION TO DISMISS STANDARD

A. Fed. R. Civ. P. 12(b)(6)

Under Fed. R. Civ. P. 12(b)(6), a complaint may be dismissed as a matter of law for two reasons: (1) lack of a cognizable legal theory; or (2) the absence of sufficient facts alleged under a cognizable legal theory. *See Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990). To survive a motion to dismiss, the complaint must "provide the 'grounds' of [plaintiff's] 'entitle[ment] to relief'", which "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do. Factual allegations must be enough to raise a right to relief above the speculative level ...." *Nichols-Stuart v. Cty. of Amador*, No. C087609, 2021 WL 3185290, at *4 (Cal. Ct. App. July 28, 2021), *review denied* (Oct. 20, 2021), *cert. denied sub nom. Nichols-Stuart v. Cty. of Amador, California*, 142 S. Ct. 2871 (2022) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555 (2007)).

1. The *Twombly* and *Iqbal* Pleading Standards

Under Rule 8, "a plaintiff's obligation to provide the 'grounds' of his 'entitle[ment] to relief' requires more than labels and conclusions, and *a formulaic recitation of the elements of a cause of action will not do*." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) ("*Twombly*") (emphasis added). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) ("*Iqbal*"). To that point, pleadings that contain "no more than conclusions ... are not entitled to the assumption of truth" otherwise applicable to complaints on a motion to dismiss. *Id.* at 679. Accordingly, the Court is "free to ignore legal conclusions, *unsupported conclusions*, unwarranted inferences and *sweeping legal conclusions cast in the form of factual allegations*." *Farm Credit Servs. v. Am. State Bank*, 339 F.3d 764, 767 (8th Cir. 2003) (cit. omitted; emphasis added).

A two-pronged approach is used to analyze the sufficiency of a complaint under Rule 8: (1) the Court should first identify and disregard conclusory allegations which are not entitled to the assumption of truth; and (2) it should then determine whether the remaining allegations, if taken as true, present a plausible claim for relief. *Iqbal*, 556 U.S. at 679. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the ***reasonable inference*** that the ***defendant is liable for the misconduct*** alleged." *Id.* at 678 (emphasis added). Therefore, a complaint must allege "enough facts to raise a reasonable expectation that discovery will reveal evidence of [the claim]." *Twombly,* 550 U.S. at 556 n.3. "[W]here the well-pleaded ***facts*** do not permit the court to infer more than the ***mere possibility of misconduct***, the complaint has alleged – but it has not shown – that the pleader is entitled to relief." *Iqbal*, 556 U.S. at 679 (emphasis added).

IV. ARGUMENT

A. Plaintiff Has Failed to Plausibly Allege that Prime Violated the ECPA.

Given the recent flood of pixel-related ECPA cases filed against healthcare providers, the law pertaining to those claims is relatively settled. A defendant, such as Prime, can violate the ECPA one of three ways. *See Doe, et al. v. Kaiser Permanente Health Plan, Inc., et al.* ("*Kaiser*"), No. 23-CV-02865-EMC, 2024 WL 1589982, at *8 (N.D. Cal. Apr. 11, 2024). **First,** a defendant can violate 18 U.S.C. § 2511(1)(a) by "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *Id.* **Second,** a defendant can violate 18 U.S.C. § 2511(1)(b) by "intentionally disclos[ing], or endeavor[ing] to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception

of a wire, oral, or electronic communication in violation of this subsection." *Id.* **And third**, a defendant can violate 18 U.S.C. § 2511(1)(c) by "intentionally us[ing], or endeavor[ing] to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection." *Id.*

Regardless of the ECPA subsection under which the claim is brought (18 U.S.C. §§ 2511(1)(a), 2511(1)(b), or 2511(1)(c)), there is no liability if: (1) the defendant "is a party to the communication" or (2) "one of the parties to the communication has given prior consent to such interception *unless* such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Kaiser*, 2024 WL 1589982, at *8.

Here, Plaintiff asserts claims under each of the ECPA's subsections: 18 U.S.C. §§ 2511(1)(a), 2511(1)(b), and 2511(1)(c). [Dkt. No. 1, ¶¶ 233, 237-238.] Each of those claims fails, however, because Prime was both a party to the allegedly intercepted communication and consented to the alleged interception. Plaintiff's ECPA claim must be dismissed.

1. Prime Was a Party to the Allegedly Intercepted Communication.

It is now well-settled law that were a plaintiff claims that a hospital's use of a pixel on its website resulted in the unlawful interception of the plaintiff's communications with that hospital, the hospital is a "party to the communication." *See, e.g., B.K. v. Eisenhower Med. Ctr.,* No. EDCV232092JGBKKX, 2024 WL 878100, at *5 (C.D. Cal. Feb. 29, 2024) ("It is clear from Plaintiffs' Complaint that Defendant was a party to Plaintiffs' Website communications, and Plaintiffs do not dispute this contention."); *Kaiser*, 2024 WL 1589982, at *8 (noting that "plaintiff

does not dispute" that the hospital was a party to the communication); *Okash v. Essentia Health*, No. CV 23-482 (JRT/LIB), 2024 WL 1285779, at *4 (D. Minn. Mar. 26, 2024) ("Essentia's alleged interception was not unlawful because it was a party to the communication."); *Williams v. Dukehealth*,, No. 1:22-CV-727, 2024 WL 898051, at *8 (M.D.N.C. Mar. 1, 2024), *report and recommendation adopted sub nom. Naugle v. Duke Univ. Health Sys., Inc*., No. 1:22-CV-727, 2024 WL 1307216 (M.D.N.C. Mar. 27, 2024) ("Defendant was a party to the communications Plaintiff alleges it subsequently disseminated.")

Because Prime was a party to the communications that Plaintiff alleges were unlawfully intercepted, Prime could not have violated the ECPA by intercepting those communications itself. *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 607 (9th Cir. 2020) (holding that the ECPA "contain[s] an exemption from liability for a person who is a 'party' to the communication, whether acting under the color of law or not."); *In re Google Inc. Cookie Placement Consumer Priv. Litig*., 806 F.3d 125, 143 (3d Cir. 2015) ("[T]he intended recipient of a communication is necessarily one of its parties[.]").

The question thus becomes: did Prime "procure any other person to intercept or endeavor to intercept" Plaintiff's communications with Prime? The answer to that question is no.

2. Prime Consented to the Use of Pixels on Its Websites.

The ECPA makes clear that liability will only attach to an interception when ***none of the parties*** to the communication have consented. *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d at 135 ("[O]rdinarily, no cause of action will lie against a private person …['']where one of the parties to the communication has given prior consent to such interception.'" (quoting 18 U.S.C. § 2511(2)(2)); *In re Grp. Health Plan Litig.*, No. 23-CV-267 (JWB/DJF), 2023 WL 8850243, at *7 (D. Minn. Dec. 21, 2023) (holding that if the "defendant is the intended recipient of

a communication…, then they are 'necessarily one of its parties' and 'have done nothing unlawful under the Wiretap Act,' even when they procured the conversation through a fraud in the inducement or through deceit'").

Clearly, here, one of the parties to the communication—Prime—consented to the use of pixels on its websites. Plaintiff herself alleges that Prime "installed tracking technologies on its Web Properties *to collect and disclose their Private Information to unauthorized third parties for its own pecuniary gain*." [Dkt. No. 1, ¶ 8 (emphasis added).] Therefore, there can be no question that Prime consented to the alleged interception of the communications between Plaintiff and Prime.

3. The ECPA's "Crime-Tort" Exception Does Not Apply.

Even with Prime being a party to the allegedly intercepted communication and even with Prime consenting to the alleged exception, Prime acknowledges that it can still be held liable under the ECPA if Prime "act[ed] 'for the purpose of' committing any crime or tort in violation of state or federal law." *In re Grp. Health Plan Litig.*, No. 23-CV-267 (JWB/DJF), 2023 WL 8850243, at *8 (D. Minn. Dec. 21, 2023) (quoting 18 U.S.C. § 2511(2)(d)).

That does not mean, however, that the crime-tort exception applies if the actual act of interception was criminal or tortious. Courts have held that, for the crime-tort exception to apply, the "criminal or tortious purpose must be ***separate and independent from the act of the recording***." *Planned Parenthood Fed'n of Am., Inc. v. Newman*, 51 F.4th 1125, 1136 (9th Cir. 2022), *cert. denied sub nom. Ctr. for Med. Progress v. Planned Parenthood Fed'n of Am.*, 144 S. Ct. 263, 217 L. Ed. 2d 113 (2023), *and cert. denied sub nom. Merritt v. Planned Parenthood Fed'n of Am., Inc.*, 144 S. Ct. 87, 217 L. Ed. 2d 20 (2023), *and cert. denied*, 144 S. Ct. 88, 217 L. Ed. 2d 20 (2023), *and cert. denied sub nom. Rhomberg v. Planned Parenthood Fed'n of Am., Inc.*, 144 S. Ct. 88, 217 L. Ed. 2d 20 (2023), *and cert. denied sub nom. Ctr. for Med. Progress v. Planned Parenthood Fed'n of Am.*, 144 S. Ct. 263, 217 L. Ed.

2d 113 (2023), *and cert. denied sub nom. Merritt v. Planned Parenthood Fed'n of Am., Inc*., 144 S. Ct. 87, 217 L. Ed. 2d 20 (2023), *and cert. denied*, 144 S. Ct. 88, 217 L. Ed. 2d 20 (2023), *and cert. denied sub nom. Rhomberg v. Planned Parenthood Fed'n of Am., Inc*., 144 S. Ct. 88, 217 L. Ed. 2d 20 (2023) (emphasis added). In other words, for the crime-tort exception to apply, the purpose of the interception must be to commit some subsequent crime or tort. *See Sussman v. Am. Broad. Companies, Inc.,* 186 F.3d 1200, 1202 (9th Cir. 1999) (finding crime-tort exception inapplicable because the plaintiffs did not allege that the "tape was made for the purpose of committing some other subsequent crime or tort"); *Caro v. Weintraub,* 618 F.3d 94, 99–100 (2d Cir. 2010) ("At the time of the recording the offender must intend to use the recording to commit a criminal or tortious act. Merely intending to record the plaintiff is not enough."). Indeed, "[i]f, at the moment [the alleged offender] hits 'record,' [he] does not intend to use the recording for criminal or tortious purposes, there is no violation." *Caro,* 618 F.3d at 99–100. "But if, at the time of the recording, the offender plans to use the recording to harm the other party to the conversation, a civil cause of action exists under the Wiretap Act." *Id.*

In short, for the crime-tort exception to apply here, Plaintiff must allege that, at the time her communications with Prime were intercepted, Prime *intended* to use the intercepted communications for a *separate and independent* crime or tort. Plaintiff has failed to do so.

As an initial matter, Plaintiff has not identified a single crime or tort separate and independent from Prime's alleged interception of the communications. Plaintiff claims that Prime violated section 42 U.S.C. § 1320d-6(a)(3) of the Health Insurance Portability and Accountability Act ("HIPAA") by "disclosing individually identifiable health information (IIHI) to a third party." [Dkt. No. 1, ¶ 240.] This is not a crime "separate and independent" from the interception; it is a crime *based* on the interception. *Kaiser*, 2024 WL 1589982, at *10 (rejecting argument that HIPAA

violation satisfies the crime-tort exception because the argument "is contrary to *Sussman* which holds that the act of interception itself cannot be the crime or the tort"). Plaintiff herself claims that the alleged interception in violation of the ECPA and the alleged disclosure in violation of HIPAA are one in the same. [Dkt. No. 1, ¶¶ 11 ("The pixels—which are configured by the website owners, here, Prime Healthcare—collect and ***transmit information from Users' browsers to unauthorized third parties***, including, but not limited to, Facebook." (emphasis added)), 9 ("The ***collection and transmission of this information is instantaneous***, invisible and occurs without any notice to—and certainly no consent from—the Users." (emphasis added), 22 ("[W]hen a User uses Prime Healthcare's Web Properties where tracking technologies, such as the Facebook Pixel are present, ***the Pixel transmits the contents of their communications to Facebook***, including, but not limited to: (i) accessing the patient portal; (ii) the exact text of the User's search queries; (iii) medical services and treatments sought; (iv) scheduling of appointments; (v) accessing and viewing the bill page; (vi) the text of URLs visited by the User; and (vii) other information that qualifies as PII and PHI under federal and state laws." (emphasis added)), 23 ("Prime Healthcare effectively planted a bug on Plaintiff's and Class Members' web browsers and ***caused them to unknowingly disclose their private, sensitive and confidential health-related communications to Facebook***." (emphasis added)).]

Even if Prime's alleged HIPAA violation were a separate and independent tort and crime, the tort-crime exception would still not apply because Plaintiff has not alleged sufficient facts to establish the HIPAA violation. § 1320d-6(a)(3) of HIPPA makes it unlawful to knowingly "disclose[] individually identifiable health information to another person." "Disclose" is the key word. Although HIPAA does not define the term "disclose," courts have defined the term as it is used in other, similar statutes. For example, on two separate occasions, the California Court of

Appeal has been called upon to interpret "disclosure" under the California Medical Information Act ("CMIA"), a California statute intended to protect confidential medical information. In both instances, the court found that a "disclosure" occurs when a medical provider gives medical information to an unauthorized third party through "an affirmative act of communication." *See Regents of Univ. of California v. Superior Ct.,* 220 Cal. App. 4th 549, 564, 163 Cal. Rptr. 3d 205, 216 (2013)*, as modified on denial of reh'g* (Nov. 13, 2013)*; Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1555–56 (2014) (stating that, in the context of the CMIA, a "disclosure" "occurs when the health care provider affirmatively shares medical information with another person or entity").

Plaintiff's own allegations belie her claim that Prime "disclosed" her confidential information to any third party. Plaintiff does not allege that Prime "affirmatively communicated" her information to third parties; she repeatedly alleges that the third parties "intercepted" her information. [Dkt. No. 1, ¶¶ 11 (alleging that "[t]he pixels…collect and transmit information"), 24 (alleging that her "information" was "intercepted by the Pixels and third-party tracking technologies"), 19 ("[T]he Pixel collects and discloses a substantial 'data packet'").] Plaintiff also alleges that her confidential information was sent *directly* to third parties from her own computer, not that it was affirmatively communicated by Prime to those third parties. [*Id.* at ¶ 50 (alleging that ***Plaintiff*** "communicate[d] certain information (within parameters set by Prime Healthcare) ***directly to Facebook***—at the same time as the User's browser is sending this information to Prime Healthcare" (emphasis added)).]

To the extent Plaintiff claims that she does, in fact, allege that Prime "disclosed" her information through its use of "Facebook Conversations API and similar tracking technologies," [Dkt. No. 1, ¶ 56], that allegation has no bearing on the crime-tort exception to the ECPA. The crime-tort exception to the ECPA asks

whether the defendant "intend[ed] to use the recording [from the interception] for criminal or tortious purposes" at the time he or she intercepted the communication. *Caro v. Weintraub,* 618 F.3d 94, 99–100 (2d Cir. 2010). As it pertains to Plaintiff's "Conversions API" allegations, there was no "interception." Plaintiff herself admits that "Facebook Conversions API allow[s] ***businesses*** to send web events, such as clicks, form submissions, keystroke events and other actions performed by the user on the Website, ***from their own servers to Facebook and other third parties***." [Dkt. No. 1, ¶ 56 (emphasis added).]

Finally, and perhaps most importantly, even if the Court were to find that Plaintiff had alleged sufficient facts to establish that Prime committed a crime or tort separate and independent from the alleged interception, Plaintiff still has not alleged and cannot allege that Prime intercepted her communications "for the purpose of committing" that underlying "criminal or tortious act." *Deteresa v. Am. Broad. Companies, Inc*., 121 F.3d 460, 467 (9th Cir. 1997) (quoting 18 U.S.C. § 2511(2)(d)).

As Plaintiff repeatedly alleges, "Pixels are routinely used to target specific customers by utilizing data to build profiles ***for the purposes of retargeting***, for example, serving online advertisements to people who have previously engaged with a business's website—***and other marketing***." [Dkt. No. 1, ¶ 49 (emphasis added); *see also id.* at ¶¶ 118 ("Ultimately, the purpose of collecting user data is to ***make money***." (emphasis added)), 191 ("One of the ***primary reasons*** that Prime Healthcare decided to embed the Pixel and other tracking technologies on its Web Properties" is "to ***improve marketing*** by creating campaigns that maximize conversions and thereby ***decrease costs*** to Prime Healthcare and boost its revenue.").]

Numerous courts have held that increasing revenue and decreasing costs are not criminal or tortious endeavors. *In re Meta Pixel Healthcare Litig*., 647 F. Supp.

3d 778, 797 (N.D. Cal. 2022) ("Multiple courts in this district have found that the crime-tort exception to the Wiretap Act is inapplicable where the defendant's primary motivation was to make money, not to injure plaintiffs tortiously."); *see also In re Google Inc.Gmail Litig..,* No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 n. 13 (N.D. Cal. Mar. 18, 2014) ("[T]he tort or crime exception cannot apply where the interceptor's 'purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money.'" (*quoting In re DoubleClick Inc. Privacy Litig.*, 154 F.Supp.2d 497, 518 (S.D.N.Y.2001)).)

At bottom, Plaintiff has failed to allege sufficient facts to plausibly claim that Prime's use of the pixel violated, in any way, the ECPA. Her claim must be dismissed.[1]

V. CONCLUSION

For the foregoing reasons, Defendant Prime Healthcare Services, Inc. respectfully requests that the Court grant its Motion to Dismiss in full and dismiss Plaintiff's Complaint with prejudice.

Respectfully submitted,

Dated: April 24, 2024

BAKER & HOSTETLER LLP

By: */s/ Matthew D. Pearson*
MATTHEW D. PEARSON

Attorney for Defendant
PRIME HEALTHCARE SERVICES, INC.

4881-6874-8983.6

[1] To the extent Plaintiff tries to argue that, even if she cannot establish a violation under 18 U.S.C. § 2511(1)(a), she still might be able to prove a violation under 18 U.S.C. § 2511(1)(b) or (c), she is wrong. 18 U.S.C. § 2511(1)(b) and (c) both require a finding that an unlawful interception occurred. Because Prime was a party to the communication and because the crime-tort exception does not apply, no unlawful interception ever occurred. Therefore, there can be no violation of 18 U.S.C. § 2511(1)(b) or (c).